AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A spam filtering system comprising a computer processor executing:

one or more spam filters; and

a randomization component that randomizes scores of the filters for one or more messages based at least in part upon a hash computed to randomize the message score, the hash is computed based at least in part upon one or more features extracted from the message whose respective individual contributions to the message score exceed a threshold, thus obfuscating the functionality of the spam filter[[.]] wherein the spam filtering system making use of a sigmoid function having the formula of $finalscore = \frac{1}{1+e^{-summedscore}}$, wherein at least one of the *summedscore* value or the *finalscore* value is randomized to effectively modify spammer behavior and to mitigate reverse engineering of the filtering system.

2. (Previously Presented) The system of claim 1, the randomization component randomizing scores of the filter so that it is difficult for a spammer to determine whether a message that is close to a threshold and changes from being one of blocked or delivered, has changed due to one of the following: a modification to the message and the randomization component .

3. (Original) The system of claim 1, the randomization component comprising a random number generator that generates at least one of a random number and a pseudo-random number.

4. (Original) The system of claim 3, the randomization component comprising one or more input components whereby the one or more input components provide input to the random number generator to facilitate determining what random number to generate for a particular message.

5. (Original) The system of claim 1, the randomization component generating a random number based at least in part upon input received from one or more input components.

6. (Original) The system of claim 5, the input from the one or more input components is based at least in part on time.

7. (Original) The system of claim 6, wherein the random number generated depends on at least one of: a time of day and an increment of time; such that the number generated changes according to any one of: the time of day and a current increment of time.

8. (Original) The system of claim 5, the input from the one or more input components is based at least in part on at least one of: a user, a recipient, and a domain receiving the message.

9. (Original) The system of claim 8, wherein the random number generated depends on at least one of: a user, a recipient, and a domain receiving the message; such that the number generated changes according to any one of: an identity of the user, an identity of the recipient of the message, and the domain receiving the message.

10. (Original) The system of claim 9, wherein the identity of any one of the user and the recipient comprises at least one of a display name and at least a portion of an email address.

11. (Original) The system of claim 5, the input from the one or more input components is based at least in part on content of the message.

12. (Original) The system of claim 11, wherein the random number generated changes depending on at least a portion of the message content.

13. (Previously Presented) The system of claim 11, wherein the hash value is used as the random number, whereby even a small change to the message content results in a substantially large change to the random number generated.

14. (Canceled)

15. (Canceled)

16. (Original) The system of claim 11, wherein a hash of a sender's IP address is computed to facilitate randomizing message scores to thereby obscure the functionality of the spam filter.

17. (Original) The system of claim 1 having a substantial effect on messages that border between spam and non-spam, whereby messages that are border-line spam are classified as spam at least part of the time by randomizing scores of the messages.

18. (Original) The system of claim 1, the randomization component mitigating spammers from finding at least one message that gets through the spam filter substantially every time it is sent.

19. - 34(Canceled)

35. (Currently Amended) A computer readable storage medium comprising computer executable instructions to carry out a method that facilitates obfuscating a spam filter comprising:

running a message through a spam filter;

computing at least one score associated with the message;

randomizing the score of the message before classifying the message as spam or non-spam by adding at least one of a random number or a pseudo-random number to the score of the message, the number added to the score of the message depending at least in part upon a hash of at least a portion of one or more features extracted from the message having respective

contributions to the score greater than zero, the at least one score associated with the message comprises a *finalscore* and a *summedscore* wherein the *finalscore* is a sigmoid function of the *summedscore* having the formula of $finalscore = \frac{1}{1+e^{-summedscore}}$, wherein at least one of the *summedscore* value or the *finalscore* value is randomized to effectively modify spammer behavior and to mitigate reverse engineering of the filtering system.; and

classifying the message as spam or non-spam.

36. (Canceled)

37. (Previously Presented) The method of claim 0, wherein the *summedscore* is a sum of all scores associated with the one or more features extracted from a message.

38. (Currently Amended) The method of claim 0, wherein the *finalscore* ~~is a sigmoid function of the *summedscore* and~~ corresponds to a value between 0 and 1 that indicates a probability that a message is spam or not.

39. (Canceled)

40. (Previously Presented) The method of claim 35, the number added to the score of the message depending at least in part upon at least one of the following:

a time of day; and

a time increment.

41. (Previously Presented) The method of claim 35, the number added to the score of the message depending at least in part upon at least one of the following:

a user;

a recipient of the message;

a domain receiving the message;

a domain of the sender; and

a machine name running the filter.

42. (Previously Presented) The method of claim 35, the number added to the score of the message depending at least in part upon contents of the message.

43. (Canceled)

44. (Previously Presented) The method of claim 35, wherein the features used to compute the hash can randomly or non-randomly change depending on at least one of a time of day and a time increment.

45. (Previously Presented) The method of claim 35, the number added to the score of the message depending at least in part upon a hash of a sender's IP address.

46. (Previously Presented) The method of claim 35, the number added to the score of the message depending on input from one or more input components.

47- 58 (Canceled)

59. (Currently Amended) A computer-readable storage medium having stored thereon the following computer executable components:

a randomization component that randomizes at least one score [[scores]] of one or more spam filters based at least in part upon a hash computed to randomize a message score, the hash is computed based at least in part upon one or more features extracted from the message whose respective individual contributions to the message score exceed a threshold, the at least one score associated with the filters comprises a *finalscore* and a *summedscore* wherein the *finalscore* is a sigmoid function of the *summedscore* having the formula of $finalscore = \frac{1}{1+e^{-summedscore}}$, wherein at least one of a *summedscore* value or a *finalscore* value is randomized thus obfuscating the functionality of a the spam filters so as to hinder reverse engineering the one or more spam filters.

60. (Canceled)

61. (Original) The computer-readable medium of claim 59, the randomization component comprising a random number generator that generates at least one of a random number and a pseudo-random number.

62. (Currently Amended) A system that facilitates obfuscating a spam filter comprising:

a means for running a message through a spam filter;

a means for computing at least one score associated with the message;

a means for randomizing the score of the message by modifying the score with at least one of a random number or a pseudo-random number, the number modifying the score of the message depending at least in part upon a hash of at least a portion of one or more features extracted from the message having respective contributions to the score greater than zero, the score of the message comprises a *finalscore* and a *summedscore* wherein the *finalscore* is a sigmoid function of the *summedscore* having the formula of $finalscore = \frac{1}{1+e^{-summedscore}}$, wherein at least one of the *summedscore* value or the *finalscore* value is randomized before classifying the message as spam or non-spam; and

a means for classifying the message as spam or non-spam.

63. (Canceled)